UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,787	03/23/2005	Rached Ksontini	90500-000043/US	6287

30593 7590 06/09/2008

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/528,787	KSONTINI ET AL.	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03-23-05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim 1 is objected to because of the following informalities: Claim 1 recites "decrypting this cryptogram the first device;" this should be changed to "decrypting this cryptogram in the first device." Appropriate correction is required.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Additionally, claim 1 recites "storing in the first device the pairing data with the second device." It is unclear where the pairing data is being stored.

Claim 3 recites the limitation "a secret key common to the second devices." There is insufficient antecedent basis for this limitation in the claim. Claim 1, upon which claim 3 depends, identifies a single "second device."

Claims 8 and 9 each recites "wherein it comprises the steps of." It is unclear as to what "it" refers to. For the sake of examination, it is assumed that "it" refers to the "Pairing Control" method.

Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marino et al (U.S. Pat 6026165 A), hereinafter referred to as Marino, in view of Candelore (U.S. Pat Pub 2002/0041337 A1), hereinafter referred to as Candelore, in further view of Terao et al (U.S. Pat Pub 2001/0005682 A1), hereinafter referred to as Terao.

Re claim 1: Marino teaches a pairing Control method between a first device such as a removable security module and a second device such as a host apparatus this pairing aiming to secure the data exchange with the aid of a unique pairing key (Abstract: lines 1-8; col 3, lines 24-29), this method comprising the steps of:

verifying the pairing between the two devices and using the unique pairing key if the pairing has been already carried out (Fig 3, elts 30, 42 & "SEARCH DEVICE ID;" col 7, line 66 – col 8, line 7), if not, searching for a free location among the locations reserved for the pairing data in the first device and in this case (col 8, lines 17-23; col 9, lines 20-28),

initiating a pairing procedure by transmitting a cryptogram contained in the second device, and comprising an identifier belonging to this device (Fig 2: elt 30 & "TO RF XMTR;" Fig 3: elt "FROM RF RCVR" & 30; col 7, lines 3-13), and extracting from this cryptogram the identifier of the second device (Fig 3: elts 30, "LOAD DEVICE ID" & "SEARCH DEVICE ID"), storing in the first device the pairing data with the second device (Fig 3, elt 42; col 7, line 51 – col 8, line 13).

While Marino teaches this cryptogram being encrypted by a secret key (Fig 4; col 8, lines 24-40), Terao teaches this cryptogram being encrypted by a secret key common to all the first devices and decrypting this cryptogram the first device (¶50-52).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Marino with the teachings in Terao, for the purpose of providing a plurality of devices with a commonly used key for transmitting data; it further ensures communicability and compatibility between a plurality of commonly owned portable devices.

The combination of Marino and Terao are silent to generating a pairing key based on this identifier. However Candelora teaches generating a pairing key based on this identifier (Fig 4, all elts; ¶21)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Marino and Terao with the teachings of Candelora as generating keys from unique device id's is commonly performed in the art for the purpose of hiding the actual keys from the devices without

actually storing the keys. All references are analogous art as they teach transmission of data from a first device to a second device using device dependant information.

Re claim 2: The combination of Marino, Terao and Candelore teaches the pairing key is based on the identifier of the second device and on the data of the first device (Candelora: ¶20).

Re claim 3: The combination of Marino, Terao and Candelore teaches the cryptogram is stored in the first device and encrypted with a secret key common to the second devices (Marino: col 2, lines 5-8; Terao: Fig 4; col 8, lines 24-40).

Re claim 4: The combination of Marino, Terao and Candelore teaches each location includes an activity counter updated during every positive verification of the pairing based on this location, the search for the location to be replaced being determined by the value of the activity counter (Marino: col 7, lines 42-44, lines 54-56 & lines 64-65; col 8, lines 7-15; col 9, lines 19-27).

Re claim 5: The combination of Marino, Terao and Candelore teaches the pairing is conditioned by the introduction of a secret code transmitted to the first device and verified by said first device (Marino: col 7, lines 42-44, lines 54-56 & lines 64-65; col 8, lines 7-15; col 9, lines 19-27). While Marino teaches this verification on the second device, the Examiner holds that it would have been obvious to one of ordinary skill in the art at the time the invention was made to off-load certain verification responsibilities to the client for the purposes of reducing the work-load of the serving entity.

Re claim 6: The combination of Marino, Terao and Candelore teaches the secret code belongs to and is unique to each first device (Marino: Fig 2, elt 32: col 7, lines 29-41).

Re claim 7: The combination of Marino, Terao and Candelore teaches the required secret code is different in each pairing (Marino: col 7, lines 41-44).

5. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marino et al (U.S. Pat 6026165 A), hereinafter referred to as Marino, Candelore (U.S. Pat Pub 2002/0041337 A1), hereinafter referred to as Candelore and Terao et al (U.S. Pat Pub 2001/0005682 A1) hereinafter referred to as Terao, in further view of Tello (U.S. Pat 6463537 B1), hereinafter referred to as Tello.

Re claim 8: Tello teaches it comprises the steps of: transmitting a unique identifier of the first device and a unique identifier of the second device to a management centre, verifying the conformity of this pairing and calculating by means of the management centre the corresponding secret code on the basis of the two identifiers, transmitting this secret code to the user, initiating the pairing and requesting the introduction of the secret code, by means of the first device, calculating by means of the first device the necessary secret code on the basis of the identifiers of the first and second devices, comparing the calculated code with that which has been introduced by the user, accepting the pairing if the two codes are identical (Fig 1; col 17, line 52 - col 18, line 3; col 18, lines 32-39; col 24, lines 25-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Marino, Terao and Candelore with the teachings of Tello for the purpose of providing a manager for verifying the two devices are allowed to inter-connect. All references are analogous art as they teach transmission of data from a first device to a second device using device dependant information.

Re claim 9: The combination of Marino, Terao, Candelore and Tello teaches it comprises the steps of determining the new secret code on the basis of the two identifiers and of an index that represents the number of pairings previously carried out, whereas the first device stores this index in its memory (Marino: Fig 2, elt 32 and Fig 3, elt 33).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat 5412718 A teaches using device ID's to generate keys

U.S. Pat Pub 2002/0124176 A1 teaches exchanging ID info and random challenges.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135